APPENDIX B
(CFO/046/10)

ICT (Information Communication and Technology)

Asset Management Plan

2010/2015

Document Control Sheet

Project Title	Asset Management Procedures
Report Title	ICT Asset Management Plan
Revision	5.0
Status	Draft – Kieran Timmins Updates And Page 8 Strategic approach to Asset Management included
Control Date	16th February 2010

Record of Issue

Issue	Status	Author	Date	Check	Date	Authorised	Date
1.0	Draft	Bernie Kenny	01/10	Ed Franklin	01/10	K Timmins	01/10
1.1	Draft	Bernie Kenny	01/10	Ed Franklin	01/10	K Timmins	01/10
2.0	Draft	Bernie Kenny	01/10	Ed Franklin	01/10	K Timmins	01/10
3.0	Draft	Bernie Kenny	01/10	Ed Franklin	01/10	K Timmins	01/10
4.0	Draft	Bernie Kenny	02/10	Ed Franklin	02/10		
5.0	Draft	Bernie Kenny	02/10	Ed Franklin	02/10		

Distribution

Organisation	Contact	Copies

"An Excellent Authority"

Contents

Foreword.

In line with the Authority's vision of making Merseyside a Safer, Stronger, Healthier Community; ICT is committed to a successful partnership working within the organisation and with third parties to deliver a value for money, secure, robust quality service whilst enabling continuous business led ICT Innovation.

Asset Management is a business focus for the organisation across three main asset categories: Property, ICT (Information Communication and Technology) and Transport which in turn sit under the Strategic Asset Management Plan that overarches the whole fundamentals of asset procedures. The purpose of this ICT Asset Management Plan is to explain the approach of ICT & the framework for the ICT Asset Management lifecycle.

ICT Asset Management carried out by ICT, on behalf of the Authority is done so in line with ITIL (Information Technology Infrastructure Library). ITIL is a set of best practices and processes for the management of the ICT Infrastructure and the delivery of services and support

For ICT, the physical life cycle of an ICT Asset has four distinct phases:

- Planning
- Acquisition
- Operation
- Disposal

And ICT follows five major principles:

- ICT Asset Management decisions are integrated with the strategic planning process
- ICT Asset planning decisions are based on an evaluation of the alternatives, which consider the 'life cycle' costs, benefits, and risk of ownership
- Accountability is established for ICT Asset condition, use and performance
- Effective disposal decisions are carried out in line with environment impact
- An effective control structure is established for ICT Asset Management

Further information on how ICT manages ICT Assets on behalf of the Authority can be found in the remainder of this document.

Executive Summary

Under ITIL ICT Asset Management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the ICT environment. ICT Assets include all elements of software and hardware that are found in the organisation environment.

In line with ITIL ICT Asset Management, ICT manages its assets effectively to help deliver its strategic priorities and service in line with risk, providing value for money services for the benefit of the local community:

- ICT has all of its ICT Assets recorded in a Configuration Management System. This system is a database which records details of all the ICT assets and their age, thus enabling ICT to effectively manage the lifecycle of its Infrastructure. The database where the Asset information is held is on a Service Management System called “Remedy”, and this gives the benefit of being able to link ICT Incidents, Assets and People to enable a more in depth trend analysis to be performed around ICT Asset Management decisions.

- ICT has a Service Catalogue, which outlines all the ICT services provided. Included in this the catalogue are references to the Capacity Planning, Security and Preventative Maintenance carried out on ICT Assets.

- ICT has a robust reporting process to provide systematic and timely reporting of compliance and performance to enable prompt asset-related decision-making regarding ICT Assets

- ICT has a Service Pipeline. The Service Pipeline comprises of new ICT services under development and these developments lead to new or change of use of ICT Assets. ICT has four main processes associated with the Service Pipeline.

    1. ICT Service Requests.
    2. Customer Requirements Document.
    3. Application Lifecycle Management
    4. KIM (Knowledge & Information Management) & ICT Strategy Group

    (See Section 6 for further details)

To mange the ICT Capital Asset Investment Plan:

- ICT classifies spend in to four categories:

    1. Underlying Spend
    2. ICT Project Spend
    3. IRMP (Integrated Risk Management Plan) Project Spend
    4. RCC (Regional Command and Control) Spend

- ICT has a 5 year lifecycle renewal policy for ICT hardware Assets at which point ICT Assets will be considered end of life. When an ICT Asset is highlighted as end of life, its role is reviewed and if still required a new asset will be purchased.

The 5 year proposed ICT Capital budget for Underlying Spend 2010-2015 stands at £1.7m. The key new growth request, other than spend for the year 2014/2015 is £390k to allow ICT to have a Microsoft Enterprise agreement to cover software licensing for back office ICT, for example servers and network security.

1 ICT Aims & Objectives

In line with the Authority's vision of making Merseyside a safer, stronger and healthier community the ICT Department Aims & Objectives will contribute to this vision by:

- Being a business-led ICT service, integrating ICT services, business operations, local, regional and national priorities and strategies.

- Having infrastructure(s) that is (are) robust, secure, reliable and resilient.

- Having the ability to accommodate change with an increasing focus on a sound business case, clear deliverables, resilience and sustainability.

- Adopting national standards including Information Technology Infrastructure Library (ITIL), Prince2 giving best practice in ICT Service Delivery, ICT Service Support and project management.

- Empowering and encouraging ICT professionals to learn and develop as individuals contributing to a team performance.

2 ICT Overview

MF&RS has an in-house staff team of 4 who proactively manage the £1.7m/annum contract with its ICT outsourced service provider, currently “telent” whilst also coordinating the management of non-outsourced services. ICT ensure the maintenance of vital '999' emergency response infrastructure, as well as continuing to expand the use of ICT technology in managing its resources more effectively in line with the risks facing communities of Merseyside and the organisational processes of the Authority.

ICT technology is an important enabler to MF&RS in realising potential benefits. In partnership with the ICT outsourced service provider, the strategy continues to ensure that MF&RS is an ICT enabled organisation delivering value for money, innovation and savings where appropriate without compromising quality.

The ICT Infrastructure comprises of the Administration Infrastructure with the core of the Mobilisation and Communications Control (MACC) Services Infrastructure connected via a firewall. A Service Desk, managed desktops, managed servers and professional services are provided to both the Administration and the MACC Services Infrastructures by the outsourced service provider, currently “telent”.

The Authority currently owns the ICT Assets in the ICT Infrastructure.

ICT Infrastructure covers:

- A network that connects 30 sites including the Service Headquarters (SHQ), Training Development Academy (TDA), Mobilising and Communications Control (MACC), Transport Workshop, and 26 Fire Stations.

- Equipment in Emergency response such as: -

    - Fire Appliances
    - Motorbikes
    - Boat
    - Incident Command Unit
    - Urban Search and Rescue Vehicle
    - Small Fires Unit
    - Cool Van

- 1600 Users who use 800 PCs

Key Corporate Systems: The Authority has a large number of systems. The most significant ones are:

- The Emergency Calls Response System: Fortek's Vision mobilising system linked to the BOSS management information module.

- The HR and Time Management System: Sophtlogic's pharOS system, a decision support and information technology solution for the Fire and Rescue Service.

- The Finance and Payroll System: Cedar Open Accounts & Midland Payroll used in the Finance Department.

- MapInfo Graphical Information System (GIS), which helps risk analysis.

3 ICT Asset Management

The ICT challenge is to deliver quality ICT services that meet agreed service levels whilst constantly adapting to changes in the organisations environment. At the same time, there is a need to obtain maximum value from ICT Assets and services to ensure achievement of the highest possible Return on Investment from the ICT infrastructure.

To balance these priorities, ICT has an effective Asset Management and Configuration Management strategy underpinned by a service Management software tool Remedy. Remedy provides a solid foundation for day-to-day ICT Service Support and Delivery.

Adopting a best practice, Asset Management and Configuration Management solution allows ICT to understand:

- What ICT Assets the Authority has
- Where they are located
- How well they are working
- How effectively they are supporting the business

As a result the following benefits have been realised:

- Accurate information on all ICT Assets provides ICT with the ability to deliver and support its services.
- Trend analysis can be carried out against Assets to aid Incident and Problem solving
- Improved ICT security through advanced ICT Asset control
- Improved financial planning through clear identification of all assets and their associated relationships
- Improved software license management ensuring legal compliance.
- Increased confidence in ICT Systems and ICT Services
- Increased customer satisfaction

A snapshot in time list of the Authority's Hardware ICT Assets can be found in **Appendix A - ICT Infrastructure metrics**. This list can be requested and produced from the Remedy System to give a real time view of the ICT Asset holding. On a yearly basis the list is produced for insurance calculation purposes.

The system is also used for various analytical tasks including:

- Identification of obsolete ICT Assets based on a purchase date
- Identification of current & previous ICT Asset Owners
- ICT Asset Rationalisation

All ICT Assets pass through a configuration management process where they are allocated and labelled with a unique asset reference number.

In line with ITIL, ICT has a software media library to improve the way it tracks software and performs Application Lifecycle Management. Please refer to **Appendix B – PC Software Asset List** and **Appendix C – MF&RS Corporate Applications.**

4 ICT Asset Monitoring Activities

In line with ITIL, ICT maintains an up to date Service Catalogue which outlines all the ICT services provided. Included in this the catalogue are references to the Capacity Planning, Security, and Preventative Maintenance carried out on ICT Assets.

Key Examples include:

Capacity Planning

Administrative Infrastructure: Capacity Planning

Service Description:

Since 2004 telent has undertaken capacity planning for the network and infrastructure at MF&RS.

Storage Infrastructure:

A policy exists for centralised and virtualised storage on a single storage area network (SAN) system, which is capacity managed through a Simple Network Management Protocol (SNMP). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.This system is duplicated at another site for resilience.

The Storage Area Network (SAN) pool which consists of physical disks in several arrays is logically partitioned into separate volumes for FILE & PRINT; EMAIL; ORACLE. The size of these storage volumes was calculated based 1.5 times the existing volume at the time of commissioning the SAN.

Security

Administrative Infrastructure: Security

Service Description:

The most important part of network security is physical. All access to server rooms and communication rooms is secured by numeric keypad access. These access codes should not be given to anyone other than telent support engineers and members of the ICT department.

The next level of security is on the network devices themselves. All PCs and servers are part of a Windows 2003 AD (Active Directory) domain. The Active Directory security policy requires that passwords must match or exceed complex password rules. New hardware can only be added to the Merseyfire domain using an account with Domain Administrator permissions.

Domain administrator passwords are changed frequently. Network hardware e.g. routers and switches each have a distinct password for each level of access.

Preventative Maintenance

Managed Desktop Preventative Maintenance

Service Description:

All desktops and laptops are built and configured with Sophos Anti Virus which is scheduled to run everyday.

All desktops and laptops are configured for continuous virus monitoring and anti virus file updates which are produced from the server.

Windows systems management server (SMS) is fully deployed to manage preventative maintenance on desktops including automatic updates.

Note: The full ICT Service Catalogue is too large to be an attachment but it is available on request from ICT.

5 ICT Asset Monitoring Reports

Effective ICT asset management requires a monitoring process to provide systematic and timely reporting of compliance and performance to enable prompt asset-related decision-making. ICT prepare and publish the following reports to fulfil this function.

Service Desk Support Report – Monthly

The monthly ICT Service Desk Performance Report is provided to enable telent and MF&RS (MF&RS) to review the Service Delivery of ICT for the authority, against the Service Delivery standard detail in the MF&RS Service Provision Agreement Dated April 2009.

ICT Infrastructure Usage Report – Monthly

The monthly ICT Infrastructure Report is provided to enable telent and MF&RS to review and discuss Infrastructure usage, review the top 10 users of each asset and share the information with the MF&RS Budget Holders.

Information Security Report – Monthly

The monthly Information Security report provides officers (including Senior Information Risk Owner (SIRO)) within MF&RS with relevant information that supports the Authority's Information Security Policy. It is also distributed and reviewed to the Strategic Knowledge Management and ICT Group plus the Diversity Action Group.

Problem Management Report – Bi-Annual

In line with ITIL Service Management processes, this report provides the statistical analysis and evidence that supports Problem Management.

Problem Management seeks to proactively minimise incidents by identifying and recording problems and known errors within the ICT infrastructure. Errors within ICT infrastructure can cause repeated incidents, which have an adverse effect on the business. Identifying and removing errors can reduce the number of incidents over time.

Customer Satisfaction Survey Report - Annual

Customers are canvassed annually via SNAP survey. All responses are analysed and reported back via this report for review, then actions undertaken against areas for improvement.

ICT Year End Report – Annual

This is the ICT Performance for the previous financial year

Major Incident Management Reports – Ad Hoc

Whenever a Major ICT Incident takes place, a Major Incident Management Report is produced and reviewed with a view to establishing lessons learnt and to feed back into ICT Service catalogue.

6 ICT Assets Service Pipeline

Under ITIL the Service Portfolio is an executive-level view for mapping services to business needs. It manages the services under development (sometimes referred to as the Service Pipeline), services that are in production or available for deployment, (sometimes referred to as the Service Catalogue), and those services that have ceased useful life (sometimes referred to as retired services). The Service Portfolio is useful for analysing where to invest, prioritizing and allocating resources, risk management and financial modelling

The ICT Service Catalogue has been referred to earlier in this report. With regards to the Service Pipeline MF&RS have four main processes associated with the Service Pipeline. These processes manage the new ICT services under development and the requirement for new or change of use of ICT Hardware & Software Assets

ICT Service Request

The ICT Service desk issue ICT Request forms to allow users to request simple technical changes, information, enquiries or hardware and software changes. e.g. mobile phones

For certain ICT requests, an approval route through the ICT Infrastructure manager is needed. The ICT request process is fully integrated in the Configuration Management System with all changes being documented.

ICT Customer Requirements Document

This procedure was introduced to capture all larger scale new MF&RS ICT Customer Requirements. Once the requirement has been captured and agreed it is then developed in one of the following ways:

1. Contract: The requirement is covered under the existing ICT provision contract.
2. Project/Change Control Note (CCN): MF&RS will pay telent via the contractual CCN process to meet all or part of the requirement.

3. Gainshare initiative; this means that an agreement will be made to allow telent & MF&RS to work on the requirement as a Gainshare item, with both parties then benefiting from the outcome.

4. Third party: MF&RS will contract to third party to deliver all or part of the project:

The method chosen for procurement/development will be the most efficient, delivering a value for money, secure, robust quality service whilst enabling continuous business led ICT Innovation.

On a monthly basis, the requirement list is reviewed by MF&RS Internal ICT team, telent based at MACC and telent based at Warwick. Larger and more complex projects are all managed under the Authority's standard project methodologies based on Prince2 governance.

This Customer Requirement process is now in its second year and the Key benefits have been:

- Clarity of ownership
- Clarity of requirements
- Clarity & management of cost
- Visibility and tracking progress
- Forward Planning
- Resource Scheduling
- Identifying duplicate effort across MF&RS departments and or stations
- Ability to utilise information from archive

Please refer to **Appendix D – ICT Customer Requirements Document (CRD) Index 2009/2010**

ICT Application Life Cycle Management

ICT is responsible for ensuring MF&RS has an Application Life Cycle Management strategy for all its applications. Working closely with all departments to develop and manage organisational software applications and individual department software application portfolios, agreeing and monitoring ICT application Service Level Agreements.

The main thrust of the application management strategy has been focused on three main goals.

Firstly, working with senior local application owners, to introduce and implement ITIL standards to application management within MF&RS. This means that:

- A CAB (Change Advisory Board) has been set up which will ensure that only authorised changes are deployed to the MF&RS infrastructure. This will also improve the communication between key system owners and ICT.

- ICT maintain and develop a Definitive Software Library (DSL). It will ensure that:

    - A secure compound is established in which master copies of all authorised versions of the organisation's software are stored and protected.

    - All documents pertaining to applications are stored in a central location for example number of users, location of users, contact details of suppliers and Service Level Agreements (SLAs).

- ICT set minimum release management standards which 3rd party suppliers are expected and contracted to reach.

Secondly, to ascertain what the roadmap will be for MF&RS applications to comply with RCC (Regional Command & Control) requirements. The applications manager collates the integration and application requirements that MF&RS must satisfy to ensure a smooth transition to RCC. This involves the assessment of whether Application providers will be capable of meeting the requirements of RCC in order to be a part of the MF&RS Application Roadmap.

Thirdly, working with senior and local Application owners to rationalise the Authority's Application portfolio. One notable success is the adoption of MapInfo as the Authority's GIS (Graphical Information System).

KIM & ICT Strategy Board

MF&RS ICT and Knowledge & Information Management (KIM) assist local application owners to implement various projects using Prince2 methodology where applicable. The ICT Application Manager monitors these projects and progress is presented to the Strategic Knowledge Management and ICT Group, which meets four times a year. Please refer to **Appendix E– Key Projects Update**

7 ICT Asset Capital Spend Strategy

To manage the ICT Asset Investment process ICT classifies spend in to four categories:

- Underlying Spend
- ICT Project Spend
- IRMP Project Spend
- RCC Spend

These are explained in more detail below:

	Spend	Why	Benefit
Underlying Spend	Spend on the existing ICT Infrastructure including Software, Desktops, Servers, Networks and Voice Communication e.g. upgrade of Station Switches	This spend stops the ICT Infrastructure and any software becoming out of date	More than just 'keeping' the lights on. An ICT enabled organisation whose systems are robust, secure and resilient with the ability to accommodate change
ICT Project Spend	Projects that: Deliver Authority changes Deliver Step changes in Technology e.g. Telephony	This spend delivers value for money, innovation and savings where appropriate.	ICT accommodating change with a focus on a sound business case and clear deliverables
Incident Risk Management Plan (IRMP) Project Spend	Spend on Specific IRMP Projects where ICT is a major enabler. e.g. Alerter	This spend delivers the Authority's IRMP	To make Merseyside a safer, stronger, healthier community
Regional Command and Control (RCC) Spend	Spend on Specific RCC projects where ICT is a major enabler. e.g. Replacement GIS	Spend to align the Authority's systems to RCC	Protecting public safety and increasing the nation's resilience

8 ICT Asset Replacement Policy

ICT Hardware Assets

The ICT Hardware Asset replacement policy is based on a 5 year equipment life. A 3 year equipment life was considered but the increased capital spend was deemed to be excessive at this point in time.

ICT Assets could also be replaced on an adhoc basis but this would lead to difficult budget forecasting with some years seeing larger budget increases than others.

If, however, ITIL problem management analysis identifies an ICT Hardware Asset that is repeatedly problematic, causing a break in service, the equipment would be considered for replacement before its 5 year equipment life.

ICT Software Assets

Microsoft Software: Enterprise Agreement:

Microsoft (EA) Enterprise Agreement is a volume licensing program for large organizations that have 250 or more desktop computers. The program provides a simple, flexible, and affordable way to keep up to date with the latest Microsoft software products.

A strategic decision was taken and ICT have entered into o Microsoft EA to cover software licensing for back office ICT, for example servers and network security. Microsoft Office has not been included in the Microsoft EA and any upgrades to Microsoft Office 2010 or later will be subject to a business case at the time.

Anti Virus and E-Mail Filtering:

ICT chosen anti virus software “Sophos” protects MF&RS from computer viruses and any other threats which may try to enter MF&RS Network.

ICT chosen E-Mail filtering Software “Websense” (also referred to as Surfcontrol) is used to filter email and quarentine non legitimate e-mail via the process of word detection. The words that result in the email being quarantined are recorded in a database and analysed on a monthly basis.

The licenses for the anti-virus and e-mail filtering are procured on a 3 year life cycle and prior to renewal a fit for purpose exercise is carried out.

Application Software:

ICT is responsible for ensuring MF&RS has an Application Life Cycle Management strategy for all its applications. Working closely with all departments to develop and manage organisational software applications and individual department software application portfolios, agreeing and monitoring ICT application Service Level Agreements. Please refer to: **Section 6 ICT Assets Service Pipeline**

9 Proposed ICT Asset Capital Spend 2010/2015

The 5 year Capital Budget 2010-2015 stands at £1,795,000, with the budget split in four ways.

Firstly capital spends on Underlying ICT Infrastructure (IT002, IT003, IT005, IT018, IT026 and IT030). This is the spend to renew existing ICT equipment as it becomes obsolete avoiding the ICT Infrastructure becoming out of date.

Based on a requirement to renew ICT equipment every five years and to have a software assurance in place for Microsoft products it has been calculated that a 5 year capital spend of £1,795,000 is required for Underlying ICT Infrastructure. New growth in underlying ICT Spend is highlighted in the table below, and a more detailed explanation is given on following pages.

	2010/2015 New Growth	**£761,000**	
IT002	ICT Software	**£392,000**	***£285,000:*** £57,000 per annum: Microsoft EA Agreement (Servers and Security) ***£105,000:*** 3 Year Renewal Of Anti virus and E-Mail Filtering Licenses in 2014/2015 ***£2,000:*** Underlying 5 Year Spend for Software Licences 2014/2015
IT003	ICT Hardware	**£106,000**	***£91,000:*** Underlying 5 Year Spend for Hardware 2014/2015
IT005	ICT Servers	**£205,000**	***£135,000:*** Storage Area Network (SAN) technology 5 Year Refresh 2014/2015 ***£70,000:*** Underlying 5 Year Spend for Servers 2014/2015
IT018	ICT Network	**£54,000**	***£40,000:*** Vesty Network Link 5 Year Refresh 2014/2015. ***£14,000:*** Underlying 5 Year Spend for Network 2014/2015
IT026	Operational Equipment	**£14,000**	***£14,000:*** Underlying 5 Year Spend for Operational Equipment 2014/2015
IT030	ICT Projects/Upgrades	**£5,000**	***£5,000:*** Underlying 5 Year Spend for Projects/Upgrades 2014/2015

Secondly capital spends on new projects to improve the ICT infrastructure or release organisation efficiencies.

Thirdly capital spends on projects identified to be in the Integrated Risk Management Plan (IRMP).

Fourthly capital spends on projects required to enable RCC (Regional Command and Control).

In terms of ICT projects and IRMP projects, capital spend usually occurs in the first year of the budget plan, unless it is a complex project.

What follows is a breakdown of the increased capital spends for the period 2010 to 2015.

IT002: ICT Software : Growth £390,000 plus Underlying Year 5 Spend £2,000

New Growth: Microsoft Enterprise Agreement is a volume licensing program for large organizations that have 250 or more desktop computers. The program provides a simple, flexible, and affordable way to keep up to date with the latest Microsoft software products.

The products can be split into Servers & Security and Desktop. New growth of ***£285,000*** is required to provide the Authority with an ICT Infrastructure where the back office ICT is flexible for business needs and secure for business use.

Previously the Authority had Capital provision for Enterprise Agreement which covered both Servers & Security and Desktop. At the present time the Authority agreed that a holiday from EA payments for desktop should be taken. This means we cannot upgrade to Microsoft Office Version 10 and later. When this requirement becomes a necessity, a business case will be presented by ICT.

The Antivirus and Filtering Software Licenses are purchased on a 3 year contract. These licenses are due for renewal in 2014/2015 at ***£105,000.***

IT003: ICT Hardware: No New Growth, but Underlying Year 5 Spend £91,000

No New Growth apart from 2014/2015 underlying year 5 spend: Equipment can be replaced on an adhoc basis but this leads to difficult budget forecasting with some years seeing larger budget increases than others a controlled planned replacement policy is now in place based on a 5 year equipment life.

IT005: ICT Servers: Growth £135,000 plus Underlying Year 5 Spend £70,000

New Growth: Equipment can be replaced on an adhoc basis but this leads to difficult budget forecasting with some years seeing larger budget increases than others. A controlled planned replacement policy is now in place based on a 5 year equipment life. A 3 year equipment life was considered but the increased capital spend was deemed to be excessive at this point in time. A ***£135,000*** bid for 2014/2015 is due to the requirement for a Storage Area Network (SAN) technology refresh. Key MF&RS data and information would be stored on this new platform whilst secondary information and archived data would be stored on the existing SAN.

IT018: ICT Network: Growth £40,000 plus Underlying Year 5 Spend £14,000

New Growth: The two key elements of the ICT Network are the SHQ/TDA Core Network and the Local Area Network (LAN) at each individual site.

2014/2015, Vesty Road Network 5 Year Refresh has been itemized separately. For future years this will be treated as any other individual site (2018/2019 Budget will be in the region of £130k as opposed to £90k bearing in mind individual Site usage may be reviewed).

IT026: Operational Equipment: No New Growth, but Underlying Year 5 Spend £14,000

Operational equipment includes, but is not limited to station end kit replacements, Pager/Alerter refresh and Remote Access Security FOB's.

IT030: ICT Projects/Upgrades: No New Growth, but Underlying Year 5 Spend £5,000

Small projects outside of scope of those identified as IRMP/Service Plan spends.

Please refer to **Appendix F - Capital 5 Year Plan 10-11 to 14-15 v1.**

10 Benchmarking & Standards

Merseyside Fire & Rescue Authority is part of the Chartered Institute of Public Finance and Accountancy (CIPFA) Value for Money (VfM) Indicators and Benchmarking Service. This allows us to benchmark against other Authority's it also allows us to benchmark against our previous achievements on a year on year basis.

Glossary

AD	Active Directory
CAB	Change Advisory Board
CCN	Change Control Note
CIPFA	Chartered Institute of Public Finance and Accountancy
CRD	Customer Requirements Document
DSL	Definitive Software Library
EA	Enterprise Agreement
GIS	Graphical Information System
ICT	Information Communication and Technology
IRMP	Incident Risk Management Plan
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
KIM	Knowledge and Information Management
LAN	Local Area Network
MACC	Mobilising and Communications Control
MF&RS	Merseyside fire and Rescue Service
RCC	Regional Command and Control
SAN	Storage Area Network
SHQ	Service Headquarters
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SMS	Systems Management Server
SNMP	Simple Network Management Protocol
TDA	Training Development Academy